Skim Penelitian Institusi

LAPORAN PENELITIAN

PENGUJIAN DAN ANALISA KEAMANAN WEBSITE TERHADAP SERANGAN *SQL INJECTION* (Studi Kasus : *Website* UMK)

Oleh :

Moh Dahlan, ST, MT (Ketua)
Anastasya Latubessy, S.Kom., M.Cs (Anggota)
Lelly Hidayah Anggraini, S.Kom., M.Cs (Anggota)
Mukhamad Nurkamid, S.Kom., M.Cs (Anggota)

Dibiayai oleh Anggaran Penerimaan dan Belanja
Universitas Muria Kudus Tahun Anggaran 2013/2014

FAKULTAS TEKNIK
UNIVERSITAS MURIA KUDUS

2014

HALAMAN PENGESAHAN

1. Judul Penelitian : Pengujian dan Analisa Keamanan *Website* terhadap Serangan *SQL Injection* (Studi Kasus : *Website* UMK)
2. Ketua Peneliti
   a. Nama Lengkap : Moh. Dahlan, ST., MT
   b. Jenis Kelamin : Laki-laki
   c. Pangkat/Golongan/NIS : Pembina/IV-a/0610701000001141
   d. Jabatan Fungsional : Lektor Kepala
   e. Fakultas/Jurusan : Teknik/Teknik Elektro
3. Anggota Peneliti : 3 orang dosen
4. Alamat KantorAlamat/Telp : Gondangmanis PO BOX 53 Bae/ 0291-438229 – Kudus
5. Jangka Waktu Penelitian : 1 Tahun
6. Pembiayaan :
   a. APB UMK 2013/2014 : Rp 6.000.000,-
   b. Sumber Lain : -

Kudus, 20 Januari 2014

Mengetahui,

Dekan Fakultas Teknik	Ketua Peneliti
Rochmad Winarso, ST, MT	**Moh. Dahlan, ST., MT**
NIDN. 0612037201	NIDN. 0601076901

Menyetujui,

Rektor	Ka. Lemlit UMK
Prof. Dr. dr. Sarjadi, SP.PA	**Drs. H. Taufik, MS, MM**
	NIDN.0011045001

Website Security Testing and Analysis of the
SQL Injection Attacks (Case Study: UMK Website)

ABSTRACT

Security is an important factor to develop a website. It has been a challenge for website developer since there is no guarantee for the definition of 'secure'. 'There is no totally secure system', is not only a statement but has been proof in reality. UMK website's is a website used for information gateway in campus. Since this website has been accessed widely, it was needed to pay attention on its security. There are some ways to test the website security like using SQL Injection. SQL injection is susceptibility when attacker has a chance to inject the Structured Query Language (SQL) through application back end. This research was aimed to found the weakness of UMK website. Those weakness would be analyzed so the solution can be used to develop secure website in the future.

Keyword: analysis, security, website, SQL injection

Pengujian dan Analisa Keamanan *Website* terhadap Serangan *SQL Injection* (Studi Kasus : *Website* UMK)

ABSTRAK

Keamanan merupakan salah satu faktor penting yang harus diperhatikan dalam membangun sebuah *website*. Hal tersebut menjadi sebuah tantangan tersendiri bagi para pengembang *website*, karena tidak ada jaminan yang pasti akan defenisi 'aman' itu sendiri. "Tidak ada sistem yang benar-benar aman", bukanlah sebuah pernyataan semata, namun telah dirasakan dalam realitas. *Website* UMK merupakan *website* yang digunakan sebagai media dan sarana informasi kampus. Mengingat *website* ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan *website*. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap kemanan *website*, salah satunya adalah dengan melakukan *SQL Injection.* SQL *injection* adalah kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi *Structured Query Language* (*SQL*) *query* yang melewati suatu aplikasi ke *database back-end*. Dengan diadakannya penelitian ini, diharapkan dapat diperoleh kelemahan dari *website* UMK. Kelemahan tersebut akan dianalisa sehingga memperoleh solusi kedepan guna pengembangan *website* yang lebih aman.

Kata kunci : analisa, keamanan, website, SQL injection

KATA PENGANTAR

Puji syukur kami panjatkan kehadirat Allah SWT., atas segala limpahan rahmat dan hidayat-Nya kami dapat menyelesaikan kegiatan laporan penelitian yang berjudul " **Pengujian dan Analisa Website terhadap Serangan SQL Injection (Studi Kasus : Website UMK)** "

Kegiatan penelitian ini dapat berjalan berkat dukungan berbagai pihak, untuk itu pada kesempatan ini kami menyampaikan terima kasih kepada:

1. Prof. Dr.dr. Sarjadi, SP.PA ., selaku Rektor Universitas Muria Kudus.
2. Rochmad Winarso, ST, MT., selaku Dekan Fakultas Teknik Universitas Muria Kudus.
3. H. Taufik MS., selaku Ketua Lembaga Penelitian Universitas Muria Kudus.
4. Unit Pelaksana Teknis Sistem Informasi Universitas Muria Kudus, dan
5. Rekan-rekan tim peneliti., terima kasih atas kerja sama tim yang baik.

Akhirnya semoga laporan penelitian ini dapat memberikan manfaat (membantu) dalam pengembangan jaringan kedepan dengan lebih baik. Tak ada gading yang tak retak, bahwa laporan ini masih jauh dari kesempurnaan dan segala saran dan kritik yang membangun sangat penyusun harapkan demi penyempurnaan laporan penelitian kedepan.

Kudus, 20 Januari 2014

Penyusun

DAFTAR ISI

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1. Latar belakang

Website adalah sebuah cara untuk menampilkan diri di *internet.* Dibaratkan w*ebsite* adalah sebuah tempat di *internet* dimana siapa saja di dunia ini dapat mengunjunginya. Keamanan merupakan salah satu indikator penting dalam membangun sebuah *website*, mengingat akses ke-*internet* yang terbuka bebas bagi masyarakat umum. Selain itu, saat ini w*ebsite* tidak hanya dijadikan layanan untuk memberikan informasi statis, tetapi telah berkembang dengan ditambahkannya fitur-fitur untuk melakukan transaksi secara *on-line*. Sampai saat ini tidak ada *website* yang dapat dikatakan benar-benar aman.

Website UMK (Universitas Muria Kudus) dengan domain umk.ac.id merupakan *website* yang digunakan sebagai media dan sarana publikasi informasi kampus. Mengingat *website* ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan *website*. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap kemanan *website*. Salah satunya adalah dengan melakukan *SQL Injection.*

SQL injection adalah kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi *Structured Query Language (SQL) query* yang melewati suatu aplikasi ke *database back-end*. Dengan mampu mempengaruhi apa yang akan diteruskan ke *database*, penyerang dapat memanfaatkan sintaks dan kemampuan dari *SQL*, serta kekuatan dan fleksibilitas untuk mendukung fungsi operasi *database* dan fungsionalitas sistem yang tersedia ke *database*. Injeksi *SQL* bukan merupakan kerentanan yang eksklusif mempengaruhi aplikasi *Web*, kode yang menerima masukan dari sumber yang tidak dipercaya dan kemudian menggunakan *input* yang membentuk *SQL* dinamis bisa rentan (Clarke, 2009). Kasus *SQL Injection*

terjadi ketika seorang penyerang dapat memasukkan serangkaian pernyataan *SQL* ke *query* dengan memanipulasi data input ke aplikasi (Anley, 2002).

Berdasarkan defenisi tersebut, dapat dikatakan bahwa serangan *SQL Injection* sangat berbahaya karena penyerang yang telah berhasil memasuki *database* sistem dapat melakukan manipulasi data yang ada pada *database* sistem. Proses manipulasi data yang tidak semestinya oleh penyerang dapat menimbulkan kerugian bagi pemilik *website* yang terinjeksi. Kebocoran data dan informasi merupakan hal yang fatal. Data-data tersebut dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.

Keamanan data dan informasi sangat penting dalam menjaga ketahanan sebuah *website*. Berdasarkan uraian-uraian tersebut, maka dinilai perlu untuk menguji kemanan *website* UMK terhadap serangan *SQL Injection*, serta melakukan analisa terhadap kelemahan sistem yang ada, sehingga dapat diperoleh tindakan selanjutnya untuk perbaikan sistem.

1.2. Rumusan masalah

Berdasarkan pada latar belakang yang dijelaskan sebelumnya, maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana cara melakukan pengujian terhadap keamanan *website* UMK?
2. Bagaimana melakukan analisa terhadap keamanan *website* UMK?

1.3. Tujuan penelitian

Tujuan dari penelitian ini adalah :

1. Melakukan pengujian terhadap keamanan *website* UMK.
2. Melakukan analisa terhadap hasil pengujian keamanan *website* UMK.

1.4. Manfaat penelitian

Manfaat dari penelitian ini adalah :

1. Dapat mengetahui paket-paket data yang berjalan.

2. Dapat mengetahui kelemahan *website* UMK, apakah sistem rentan terhadap serangan.
3. Dapat mengetahui langkah atau tindakan pencegahan, berdasarkan hasil analisa terhadap pengujian keamanan *website* UMK.

BAB II
TINJAUAN PUSTAKA

Beberapa penelitian terkait *forensic* jaringan antara lain, Ruchandani, dkk telah melakukan eksperimen dasar forensic jaringan dengan menangkap lalu lintas paket pada jaringan, menganalisis karakteristiknya, dan mencoba untuk mengetahui aktifitas yang berbahaya dalam membantu mengidentifikasi sumber aktivitas sebagai kerusakan yang dilakukan pada jaringan menggunakan *tools tcp-dump*, *e-thereal*, dan *n-map*. Disimpulkan bahwa *tcp-dump, ethereal*, dan *n-map* sangat ampuh untuk membantu dan menangkap dan menganalisis paket jaringan diantaranya paket sniffing dan port scanning.

Kaushik dan Joshi (2010) melakukan forensik jaringan untuk serangan ICMP. forensik jaringan adalah teknologi investigasi khusus yang menangkap, merekam dan menganalisis paket jaringan dan menentukan anomaly dalam lalu lintas apakah sebuah serangan atau bukan. Tantangan forensik jaringan adalah pengumpulan, pemeriksaan, analisis, identifikasi fitur untuk menentukan serangan dan capture paket dengan volume yang besar. Proses analisis forensik melibatkan persiapan, pengumpulan, pelestarian, pemeriksaan, analisis, investigasi dan tahap presentasi. Kaushik dan Joshi mengusulkan model sistem forensik jaringan untuk ICMP untuk mengumpulkan data jaringan, mengidentifikasi paket yang mencurigakan, memeriksa protokol dan validasi serangan. Untuk mengatasi masalah jumlah data yang besar yang akan diperiksa maka hanya digunakan informasi header paket ICMP saja dengan format paket capture: libcap dan ekstensi file pcap. Eksperimen dilakukan menggunakan nmap, sing dan traceroute.

Beberapa penelitian terkait yang membahas tentang SQL Injection adalah, Halfond dan Orso (2005) menyajikan dan mengevaluasi teknik baru untuk mendeteksi dan mencegah serangan *SQL Injection*. Teknik menggunakan pendekatan berbasis model untuk mendeteksi *query* illegal sebelum dieksekusi

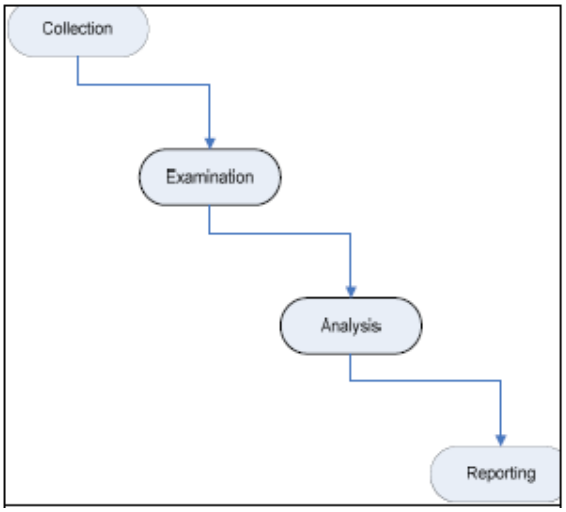
pada basis data. Halfond dan Orso (2005) mengembangkan alat AMNESIA (*Analysis and Monitoring for NEutralizing SQLInjection Attacks*) yang menerapkan teknik secara statis dan dinamis untuk mengevaluasi teknik pada aplikasi *web*. Teknis statis menggunakan analisis program untuk membangun model *query* yang sah yang dapat dihasilkan aplikasi, sedangkan teknik dinamis menggunakan pemantauan *runtime* untuk memeriksa yang dihasilkan *query* dan memeriksa model statis yang dibangun. Halfond dan Orso (2005) mengusulkan model baru untuk melawan SQLIA yaitu kerentanan yang disebabkan oleh input pengguna yang tidak divalidasi dengan menggunakan kombinasi teknik analisis statis dan dinamis dan menerapkannya pada alat *prototype* AMNESIA.

Pomeroy dan Tan (2011) membahas mengenai tantangan rekaman jaringan dan manfaat penggunaannya di masa depan. Solusi perekaman adalah untuk mendeteksi dan mengungkap serangan. *SQL Injection* merupakan salah satu serangan teratas selain XSS (*Cross Site Scripting*) dari tahun 2002 hingga tahun 2008. Cara untuk meningkatkan rekonstruksi serangan *web* adalah memahami dan memperbaiki kelemahan aplikasi *web* serta dukungan hukum pidana dan perdata. *Firewall* tidak efektif untuk memblokir lalu lintas sedangkan IDS (*Intrusion Detection System*) untuk memicu perekaman aplikasi jaringan yang dapat meningkatkan efektifitas rekonstruksi serangan *SQL Injection.*

Penelitian yang akan dikerjakan saat ini, akan membahas tentang serangan *SQL Injection*, dengan melakukan pengujian terhadap sistem keamanan *website* Universitas Muria Kudus. *Tools* yang digunakan adalah *Havij*, dimana *Havij* adalah *SQL Injection tools* otomatis yang membantu pengujian penetrasi untuk menemukan dan mengeksploitasi kerentanan *SQL Injection* pada halaman *web*.

BAB III
METODE PENELITIAN

Pada penelitian ini metodologi yang digunakan secara garis besar menggunakan dua pendekatan, yaitu pendekatan proses forensik untuk menganalisa teknis keamanan website dan studi pustaka sebagai referensi kajian dan teori dalam melakukan observasi terkait tema penelitian. Metode dalam pelaksanaan kegiatan ini dapat ditunjukkan pada diagram alir pada gambar 3.1.



Gambar 3.1. Diagram Alir Penelitian (Baryamureeba dan Tushabe, 2004)

3.1. Metode Pendekatan Proses Forensik

Tahapan-tahapan yang digunakan dalam proses forensik antara lain :

1. Identifikasi (*Collection*)

   Pada tahap ini dilakukan identifikasi terhadap kebutuhan-kebutuhan, baik kebutuhan fungsional sistem maupun identifikasi kondisi jaringan *website* Universitas Muria Kudus. Pada tahapan identifikasi ini tim peneliti berhasil mengidentifikasi kebutuhan alat dan bahan, identifikasi veriabel yang diteliti, jangka waktu penelitian dan tempat penelitian.

   a Alat dan Bahan

      1) Satu buah komputer sebagai IDS Snort Server
      2) Tools IDS Snort

3) Tools Wiresark
4) OS Linux (Ubuntu)

b Waktu Penelitian : Juni 2013-Januari 2014

c Tempat Penelitian : Pusat Sistem Informasi UMK

d Variabel yang di teliti : Website UMK

2. Pengujian (*Examintaion*)

   Pada tahap ini mulai dilakukan pengujian terhadap keamanan *website* Universitas Muria Kudus (UMK). Peneliti mulai melakukan SQL *Injection* terhadap *website* UMK. Serangan disini hanya dilakukan untuk melihat apakah penyerang dapat memasuki *database website* UMK tanpa melakukan manipulasi terhadap *database* yang ada, sehingga tidak akan mengganggu kondisi *website* yang sedang berjalan.

3. Analisa (*Analysis*)

   Pada tahapan ini, dilakukan analisa terhadap hasil serangan SQL *Injection*, hal ini berguna untuk menemukan kelemahan-kelemahan pada *website* UMK. Berdasarkan hasil analisa, juga diharapkan dapat diperoleh solusi untuk pengembagan keamanan sistem.

4. Pelaporan (*Reporting*)

   Pada tahap pelaporan, mulai dilakukan dokumentasi terhadap hasil penelitian beserta analisisnya.

3.2. Metode Pengumpulan Data

Dalam menyusun penelitian ini, kegiatan pengumpulan data dilakukan dengan beberapa cara antara, antara lain:

1. *Library Research*

   Pengumpulan data dilakukan dengan mempelajari bahan-bahan tertulis berupa buku, *browsing* melalui internet terhadap masalah yang berkaitan.

2. *Interview* dan Observasi

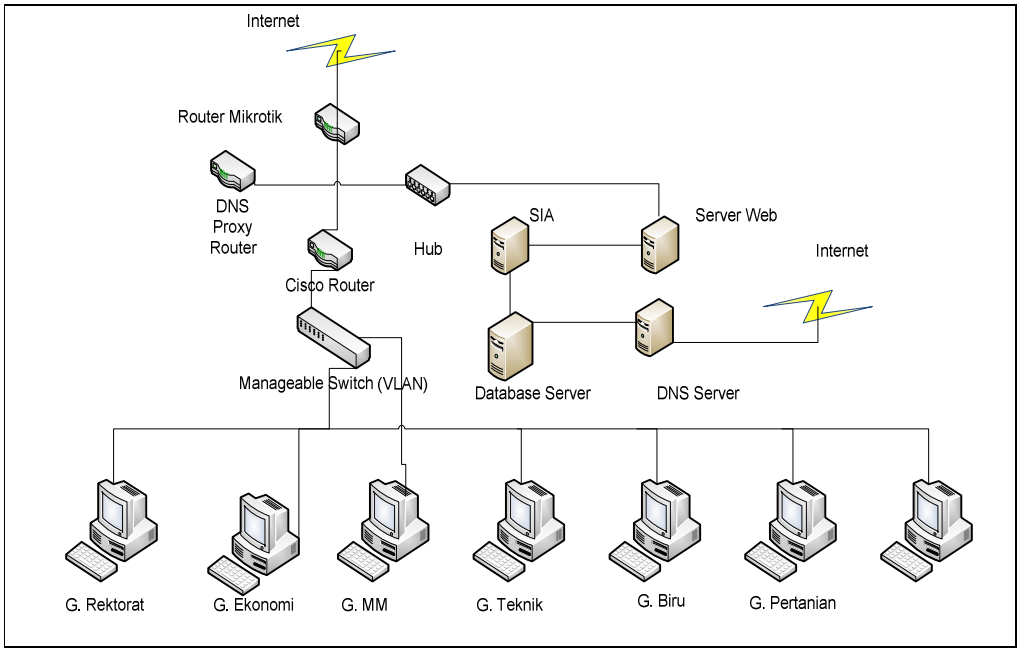
   Pada teknik ini penulis memperoleh data-data yang memiliki relevansi dengan penelitian dengan langsung melakukan observasi virtual dan nonvirtual. Virtual dengan mengunjungi *website* umk.ac.id, sedangkan

nonvirtual dengan langsung mengunjungi Unit Pelaksana Teknis Sistem Informasi (UPT SI) Universitas Muria Kudus untuk mendapatkan informasi yang relevan.

BAB IV
HASIL DAN PEMBAHASAN

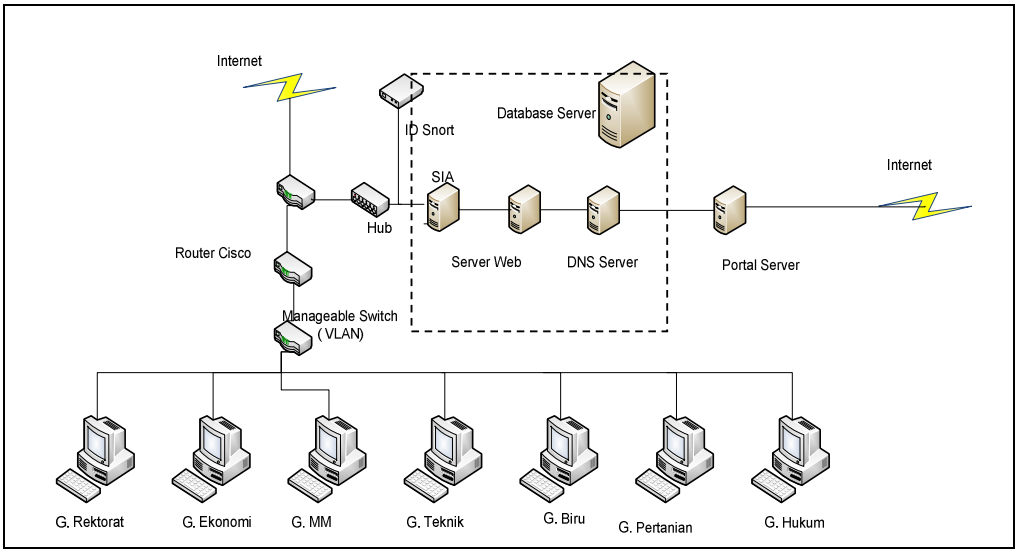
4.1. Perbandingan Topologi Jaringan UMK

Jaringan *intranet* UMK adalah jaringan yang menghubungkan komputer-komputer yang tersebar dilingkungan Universitas Muria Kudus baik yang terhubung secara *local area network* (LAN) maupun terhubung secara *offline* menggunakan fasilitas *dial-up.* Pusat jaringan (*backbone*) *intranet* terletak di Unit Pelaksana Teknis Perencanaan Sistem Informasi (Nurkamid, 2011). Topologi Jaringan yang berjalan pada jaringan di Universitas Muria Kudus dapat dilihat seperti yang terdapat pada Gambar 4.1. Dalam hal ini server DNS, proxy, dan mikrotik router dipisahkan secara *hardware,* sehingga beban kerja pada *proxy server* menjadi terpisah.



Gambar 4.1. Topologi Jaringan UMK Sebelum Penelitian

Dalam penelitian ini, ditambahkan sebuah *server* untuk IDS Snort. Server IDS Snort ini diletakan didepan jaringan internet, sebelum *web server* sistem. Dengan penambahan *server* IDS Snort seperti yang ditunjukan pada Gambar 4.2 maka semua paket data yang akan masuk ke *web server* UMK dapat dipantau.



Gambar 4.2. Topologi Jaringan UMK Setelah Penambahan IDS *Server*

4.2. Implementasi IDS Snort

Penelitian ini dilakukan dengan menambahkan sebuah komputer *server* yang bertindak sebagai IDS Snort. *Intrusion Detection System* (IDS) adalah sejenis perangkat lunak yang berfungsi untuk mendeteksi intrusi sistem. Instrusi disini adalah menganalisa segala macam serangan yang mungkin terjadi dari luar sistem. Gambar 4.3 menunjukkan hasil implementasi dari *server* IDS Snort yang diletakan pada Pusat Sistem Informasi (PSI) Universitas Muria Kudus.

Gambar 4.3. IDS *Server* di Pusat Sistem Informasi UMK

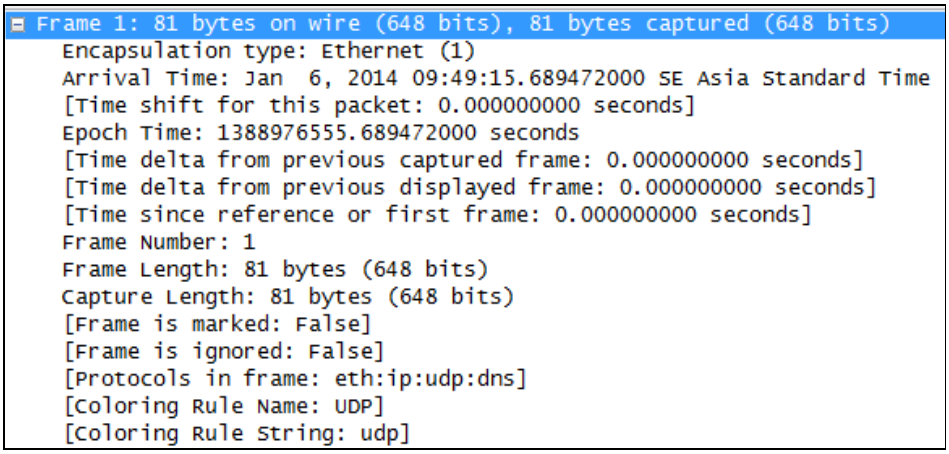
4.3. Hasil Analisa Paket Data IDS Snort

Server yang diletakan di PSI dipantau selama kurang lebih satu bulan, banyak sekali paket data yang mengalir. Terdapat beberapa paket data yang mengalir merupakan ancaman, sehingga IDS akan memberikan warning (*alert*). Beberapa *alert* yang muncul pada IDS Snort seperti yang ditunjukan pada Gambar 4.4. Baris pertama sampai baris kelima pada Gambar 4.4 menunjukan adanya *false postif*, merupakan gejala yang sebenarnya tidak ada. Sehingga tidak terlalu berbahaya. Baris 7 sampai baris 8 menunjukan adanya pengintaian yang melihat apakah ada celah yang terbuka.

```
1  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
2  [Classification: Attempted Denial of Service] [Priority: 2]
3  01/06-06:44:50.070725 192.168.1.3 -> 198.52.235.98
4  UDP TTL:64 TOS:0x0 ID:16758 IpLen:20 DgmLen:820
5  Frag Offset: 0x039D   Frag Size: 0x0320
6
7  [**] [123:8:1] (spp_frag3) Fragmentation overlap [**]
8  [Priority: 3]
9  01/06-06:44:50.843844 192.168.1.3 -> 198.52.235.98
10 UDP TTL:64 TOS:0x0 ID:53652 IpLen:20 DgmLen:820
11 Frag Offset: 0x039D   Frag Size: 0x0320
```

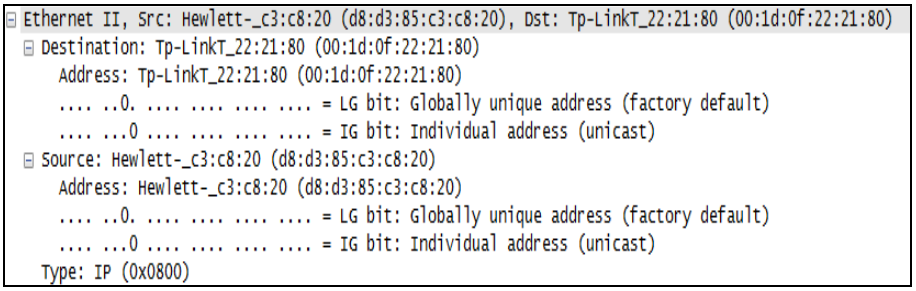
Gambar 4.4. Alert pada IDS Snort

Gambar 4.5 menunjukkan salah satu frame paket data yang mengalir di jaringan. Paket data ini di-*capture* pada tanggal 6 Januari 2014, dengan panjang frame 81 bytes (648 bits). Protokol jaringan uang digunakan adalah UDP.



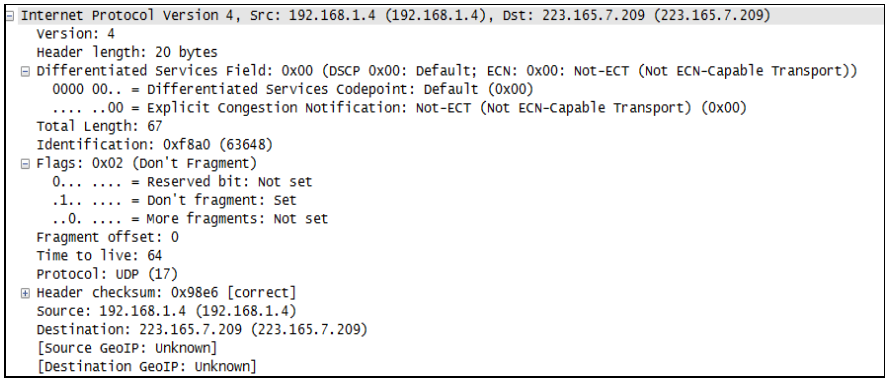
Gambar 4.5. Frame Paket Data di Jaringan

Ethernet merupakan lapisan fisik dan data link pada *local area network*. Gambar 4.6 menunjukkan ethernet yang digunakan, baik dari sumber dan tujuan paket data di jaringan.



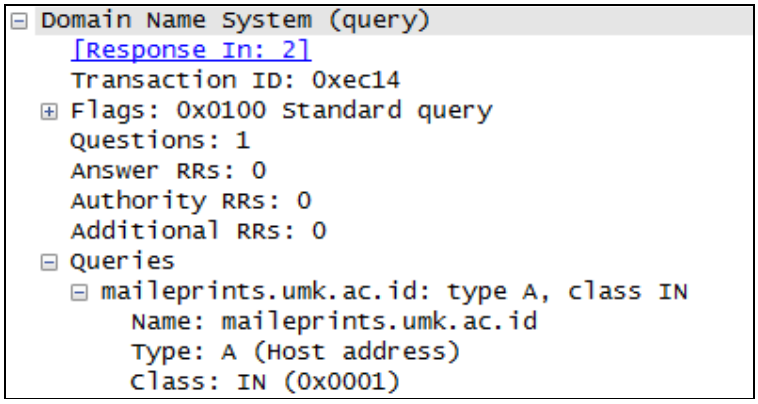
Gambar 4.6. Ethernet Paket Data di Jaringan

Paket data yang mengalir pada jaringan menggunakan IP Versi 4, dengan alamat sumber adalah 192.168.1.4 dengan tujuan 223.165.7.209. Informasi detailnya seperti yang ditunjukkan pada Gambar 4.7.



Gambar 4.7. IP Paket Data di Jaringan

Informasi Domain Name System (DNS) ditunjukkan pada Gambar 4.8. Terlihat bahwa DNS yang coba diakses adalah maileprints.umk.ac.id.



Gambar 4.8. DNS Paket Data di Jaringan

4.4. Solusi Rule yang di tawarkan

Aturan snort yang ditawarkan peneliti pada *sysadmin* dalam pengembangan selanjutnya adalah aturan snort untuk melihat adanya kemungkinan adanya serangan SQL *Injection*(varchar) seperti yang ditunjukkan pada Gambar 4.9.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"< IN >
WEB_SERVER Possible SQL Injection (varchar)";
flow:established,to_server; content:"varchar("; nocase; http_uri;
classtype:attempted-admin;
reference:url,doc.emergingthreats.net/2008175;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_SERVER/WEB_SQL_Injection_Monster_List;
sid:2008175; rev:5;)
```

Gambar 4.9. Aturan Snort tentang Possibility SQL Injection(varchar)

Menurut *rule*, apabila terdapat paket TCP dari luar melalui port apapun menuju ke dalam melalui port HTTP (80), yang sesuai dengan pola (baca keterangan *rule* 1) maka akan mengirimkan pesan "WEB_SERVER *Possible SQL Injection* (varchar)".

Keterangan *Rule* :

· alert adalah tanda peringatan.

- tcp adalah jenis protokol transport.

· $EXTERNAL_NET any adalah host asal yang melewati port manapun.

· -> adalah aliran dari host asal ke host tujuan.

· $HTTP_SERVERS $HTTP_PORTS adalah server HTTP melewati HTTP port (80).

· msg:"< IN > WEB_SERVER Possible SQL Injection (varchar)"; adalah pesan yang akan diterima apabila terjadi sebuah event.

· flow:established,to_server; adalah koneksi TCP yang terbentuk dalam host sumber ke host tujuan.

· content:"varchar("; artinya konten spresifik yang dicari

. nocase; adalah pengabaian case untuk menetapkan pola yang dicari.

· http_uri; adalah pencarian pola yang sesuai dengan konten pada normalized URI.

· classtype:attempted-admin; artinya mencoba mendapatkan hak user, ini memiliki prioritas yang tinggi.

· reference:url,doc.emergingthreats.net/2008175; reference:url,www.emergingthreats.net/cgibin/

cvsweb.cgi/sigs/WEB_SERVER/WEB_SQL_Injection_Monster_List; merupakan referensi ke sistem pengidentifikasi serangan eksternal.

- sid:2008175; merupakan id dari aturan snort.
- rev:5;) artinya revisi aturan snort ke 5.

BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan hasil identifikasi di bab pembahasan, maka penyusun dapat menyimpulkan bahwa :

1. Tidak ada sistem yang dikatakan benar-benar aman, sehingga aktifitas jaringan perlu dipantau setiap saat dengan mengamati setiap paket data yang berjalan didalam jaringan.
2. Dengan adanya *IDS Snort*, aktifitas jaringan yang berjalan di Pusat Sistem Informasi (PSI) Universitas Muria Kudus dapat dipantau secara berkala dan di analisa sebagai upaya deteksi dini terhadap serangan.
3. Pemberian aturan snort (*rule*) yang tepat dapat memberikan peringatan/*alert* sehingga serangan dari *intruder* terhadap jaringan dapat diketahui oleh *sysadmin*.

5.2. Saran

Saran yang dapat diberikan pada penelitian ini adalah:

1. *Sysadmin* pada Pusat Sistem Informasi harus dapat menentukan *rule* yang tepat pada *snort*. Sehingga dapat ditentukan aktifitas mana dijaringan yang dikatakan sebagai *intruder* dan mana yang tidak, berdasarkan *rule* yang berlaku.
2. Untuk pengembangan selanjutnya dapat memberikan solusi aturan–aturan yang lain, bukan saja terhadap *Possibility SQL injection* (*varchar*). Mengingat serangan *SQL injection* tidak hanya berupa penambahan *varchar*.

DAFTAR PUSTAKA

Anley, C., 2002, Advanced SQL Injection in SQL Server Applications. *An NGSSoftware Insight Security Research (NISR) Publications*: Next Generation Security Software Ltd.

Baryamureeba,V., Tushabe, F., 2004, The Enhanced Digital Investigation Process Model. *Proceedings of the Fourth Digital Forensic Research Workshop*, May 27.

Clarke, J., 2009, *SQL Injection Attacks and Defense*. Burlington: Syngress Publishing and Elseiver.

Halfond, W.G.J., Orso, A., 2005., AMNESIA: Analysis and Monitoring for NEutralizing SQLInjection Attacks. *IEEE and ACM Intern. Conf. On Automated Software Engineering (ASE 2005)*. Hal. 174–183, Nov. 2005.

Nurkamid, M., 2011, Analisa Keefektifan Jaringan Local Area Network (Intranet) Universitas Muria Kudus, Jurnal Sains dan Teknologi, vol. 4 no. 2, Universitas Muria Kudus, Kudus.

Pomeroy, A., Tan, Q., 2011, Effective SQL Injection Attack Reconstruction Using Network Recording. *IEEE International Conference on Computer and Information Technology*.Canada.

PERSONALIA TIM PENELITI

1. Ketua Peneliti

a. Nama Lengkap	:	Moh.Dahlan, ST., MT.
b. Jenis Kelamin	:	Laki-laki
c. NIDN	:	0610701000001141
d. Disiplin Ilmu	:	Teknik Elektro
e. Pangkat/Golongan	:	Pembina/IV-a
f. Jabatan Fungsional/Struktural	:	Lektor Kepala
g. Fakultas/Jurusan	:	Teknik/Teknik Elektro
h. Waktu Penelitian	:	12 jam/minggu

2. Anggota Peneliti 1

a. Nama Lengkap	:	Anastasya Latubessy, M.Cs
b. Jenis Kelamin	:	Perempuan
c. NIDN	:	0604048702
d. Disiplin Ilmu	:	Teknik Informatika
e. Pangkat/Golongan	:	-
f. Fakultas/Program Studi	:	Teknik/Teknik Informatika
g. Waktu Penelitian	:	12 jam/minggu

3. Anggota Peneliti 2

a. Nama Lengkap	: Lelly Hidayah A, S.Kom., M.Cs
b. Jenis Kelamin	: Perempuan
c. NIDN	: 0628038702
d. Disiplin Ilmu	: Teknik Informatika
e. Pangkat/Golongan	: -
f. Fakultas/Program Studi	: Teknik/Teknik Informatika
g. Waktu Penelitian	: 12 jam/minggu

4. Anggota Peneliti 3

a.	Nama Lengkap	:	Mukhamad Nurkamid., M.Cs
b.	Jenis Kelamin	:	Laki-laki
c.	NIS	:	0610701000001212
d.	Disiplin Ilmu	:	Teknik Informatika
e.	Pangkat/Golongan	:	Penata Muda Tk.I/III-b
f.	Jabatan Fungsional/Struktural	:	Asisten Ahli
g.	Fakultas/Program Studi	:	Teknik/Teknik Informatika
h.	Waktu Penelitian	:	12 jam/minggu

5. Pekerja Lapangan/Pencacah : 5 orang mahasiswa

DAFTAR RIWAYAT HIDUP

1. Ketua Peneliti

a.	Nama Lengkap	:	Moh. Dahlan, ST., MT.
b.	Jenis Kelamin	:	Laki-laki
c.	Fakultas/Jurusan	:	Teknik/Teknik Elektro
d.	Pangkat/Golongan/NIS	:	Pembina/IV-a/0610701000001141
e.	Bidang Keahlian	:	Teknik Elektro
f.	Alamat Kantor	:	Universitas Muria Kudus Gondang Manis PO. BOX Bae,Kudus
g.	E-mail	:	dahlan_kds@yahoo.com
h.	Pengalaman Penelitian/Publikasi	:	

1. Pemanfaatan Aplikasi Jejaring Sosial Facebook untuk Media Pembelajaran, APBU UMK (2010)

Kudus, 20 Januari 2014

Ketua Peneliti,

Moh. Dahlan, ST., MT

2. Anggota Peneliti 1

1.	Nama Lengkap	:	Anastasya Latubessy, S.Kom., M.Cs
2.	Jenis Kelamin	:	Perempuan
3.	Fakultas/Jurusan	:	Teknik/Teknik Informatika
4.	Pangkat/Golongan/NIDN	:	-/-/-
5.	Bidang Keahlian	:	Basis Data Terdistribusi, Jaringan Komputer
6.	Alamat Kantor	:	Universitas Muria Kudus Gondangmanis POBOX 53 Bae,Kudus
7.	E-mail	:	anastasyalatubessy@gmail.com
8.	Pengalaman Penelitian/Publikasi	:	

1. Penelitian, Aplikasi Rekam Medis berbasis *web* dengan *database* terdistribusi, DIKTI, 2008.
2. Publikasi Jurnal, Implementasi Sistem Interkoneksi Basisdata Terdistribusi Menggunakan Socket API (Studi Kasus : Sistem KGB), IJCCS-Vol 6 no.2 Juli 2012, UGM.

Kudus, 20 Januari 2014

Anggota Peneliti,

Anastasya Latubessy, S.Kom., M.Cs

3. Anggota Peneliti 2

1. Nama Lengkap	:	Lelly Hidayah A., S.Kom., M.Cs
2. Jenis Kelamin	:	Perempuan
3. Fakultas/Jurusan	:	Teknik/Teknik Informatika
4. Pangkat/Golongan/NIDN	:	-/-/-
5. Bidang Keahlian	:	Rekayasa Perangkat Lunak
6. Alamat Kantor	:	Universitas Muria Kudus Gondang Manis PO. BOX 53 Bae, Kudus
7. E-mail	:	anglelly14@gmail.com
8. Pengalaman Penelitian/Publikasi	:	-

Kudus, 20 Januari 2014

Anggota Peneliti,

Lelly Hidayah Anggraini, S.Kom., M.Cs

4. Anggota Peneliti 3

a.	Nama Lengkap	:	Mukhamad Nurkamid,S.Kom, M.Cs
b.	Jenis Kelamin	:	Laki-laki
c.	Fakultas/Jurusan	:	Teknik/Teknik Informatika
d.	Pangkat/Golongan/NIS	:	Penata Muda Tk.I/IIIb/0610701000001212
e.	Bidang Keahlian	:	Pemrograman dan Basisdata
f.	Alamat Kantor	:	Universitas Muria Kudus Gondang manis POBOX53 Bae, Kudus
g.	E-mail	:	nurkamid@gmail.com
h.	Pengalaman Penelitian/Publikasi	:	

1. Pemanfaatan Aplikasi Jejaring Sosial Facebook untuk Media Pembelajaran, APBU, (2010)
2. Analisa Keefektifan Jaringan Local Area Network (Intranet) Universitas Muria Kudus-APBU, (2011)
3. Penerapan Geographic Information Systems (GIS) berbasis Open Layers di PLN APJ Kudus (2012)- Seminar Nasional Ilmu Komputer "*Solusi Komputasi dan Teknologi Informasi dalam Peningkatan Daya Saing Global*" Universitas Diponegoro 2012, Prosiding Seminar Nasional Ilmu Komputer Universitas Diponegoro, ISBN: 978-979-756-841-2, 15 September 2012, hal 5.
4. Pemanfaatan Website E-commerce untuk Penjualan Produk UMKM Pada Kluster Konveksi dan Bordir di Kabupaten Kudus (2013)-Seminar Nasional Ilmu Komputer Seminar Nasional Ilmu Komputer " *Cloud Computing Security*" Universitas Negeri Semarang 2013, Prosiding Seminar Nasional Ilmu Komputer Universitas Negeri Semarang, ISBN: 978-602-14724-4-6, 23 November 2013, hal 61-63.

Kudus, 20 Januari 2014

Anggota Peneliti,

Mukhamad Nurkamid, S.Kom., M.Cs